REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
19-05-2013	FINAL	

4. TITLE AND SUBTITLE

Navy Information Dominance, the Battle of Midway, and the Joint Force Commander: It Worked Then, It Needs to Work Now

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Mitchell H. Finke, USN

Paper Advisor: Patrick C. Sweeney, PhD

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Dept.
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The changing character of warfighting from the traditional domains of air, sea, land, and to an extent space, to the Information Domain and Cyberspace, is putting increased emphasis on the need for the Joint Force Commander to employ his force to achieve Information Dominance. The information domain in warfighting is becoming increasingly relevant as nations develop capabilities to defend and operate offensively in cyberspace. The goal of Navy Information Dominance is to assist in achieving decision superiority, Assured Command and Control, Battlespace Awareness, and Integrated Fires. Navy Information Dominance aims to use information in cyberspace as a way and means in warfare; as a battery in the Joint Forcer Commander's arsenal. The principle of Navy Information Dominance and its fundamental capabilities were at play in the Battle of Midway in June 1942 proving their relevance in achieving decision superiority against an adversary. While the other services that comprise the Joint Force have Information Dominance missions, they lack a comprehensive approach to achieving Information Dominance. This paper argues the Joint Force Commander must adopt the U.S. Navy model to achieve Information Dominance to be successful in future conflicts.

15. SUBJECT TERMS

Information Dominance Corp, Cyberspace, Information Superiority, Midway

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Chairman, JMO Dept
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		18	401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Navy Information Dominance, the Battle of Midway, and Joint Force Commander: It Worked Then, It Needs to Work Now

By

Mitchell H. Finke

Lieutenant Commander, United States Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____//S//_____

19 May 2013

Contents Page

Paper Abstract

The changing character of warfighting from the traditional domains of air, sea, land, and to an extent space, to the Information Domain and Cyberspace, is putting increased emphasis on the need for the Joint Force Commander to employ his force to achieve Information Dominance. The information domain in warfighting is becoming increasingly relevant as nations develop capabilities to defend and operate offensively in cyberspace. The goal of Navy Information Dominance is to assist in achieving decision superiority, Assured Command and Control, Battlespace Awareness, and Integrated Fires. Navy Information Dominance aims to use information in cyberspace as a way and means in warfare; as a battery in the Joint Forcer Commander's arsenal. The principle of Navy Information Dominance and its fundamental capabilities were at play in the Battle of Midway in June 1942 proving their relevance in achieving decision superiority against an adversary. While the other services that comprise the Joint Force have Information Dominance missions, they lack a comprehensive approach to achieving Information Dominance. This paper argues the Joint Force Commander must adopt the U.S. Navy model to achieve Information Dominance to be successful in future conflicts.

The opening shots of the next war will likely occur in cyberspace.

- Vice Admirals Kendall Card and Michael Rogers. "The Navy's Newest Warfighting Imperative." Oct. 2012.

Introduction

Warfighting is expanding beyond the traditional domains of land, air, sea and to some degree space. The information domain, particularly cyberspace, will become increasingly important to the Joint Force Commander (JFC) to defend and when necessary, to use to conduct offensive operations. History and modern warfare is ripe with examples of defensive and offensive operations conducted in traditional disciplines; e.g., airplanes for air warfare, ships and submarines for surface and subsurface warfare, soldiers and artillery for land warfare. Because modern warfare will also be waged in the information domain, one must consider information as a warfare discipline.[1] Information superiority or Information Dominance and decision superiority are critically linked. Although dated, General Henry Shelton's explanation of information superiority in "Joint Vision 2020" from 2000 shows the concept's importance to Joint warfighting is enduring:

> Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions. The joint force must be able to take advantage of superior information converted to superior knowledge to achieve 'decision superiority'—better decisions arrived at and implemented faster than an opponent can react.[2]

The Navy's structure and principles for achieving Information Dominance, which are anchored in history and leverage the combined capabilities of sub-communities to achieve

[1] Kendall L. Card and Michael S. Rogers, Vice Admirals, USN, "Navy Strategy for Achieving Information Dominance 2013-2017: Optimizing Navy's Primacy in the Maritime Information Domains," *Public.navy.mil/fcc_c10f*, November 2012, accessed 8 March 2013, http://www.public.navy.mil/fcc-c10f/Pages/FactSheets.aspx. p. 4-5.

[2] Chairman of the Joint Chiefs of Staff (CJCS), *Joint Vision 2020*. (Pentagon, Washington D.C.: US Government Printing Office, June 2000), p. 8.

decision and information superiority, is a model the Joint Force Commander must adopt to succeed in future warfighting.

Background and Current Doctrine for Navy Information Dominance

Before one can fully understand the fundamental capabilities of Navy Information Dominance, a review of strategic and national guiding principles must be understood. National political leadership, appointed government officials, and senior military leadership have incorporated concepts of Navy Information Dominance into doctrine and guidance at multiple levels. In his Defense Strategic Guidance *Sustaining U.S. Leadership: Priorities for the 21st Century Defense* signed on 3 Jan 2012, President Obama included his primary missions for the U.S. Armed Forces. One of these states "Operate Effectively in Cyberspace and Space…the Department of Defense will…invest in the capability to defend networks, operational capability, and resiliency in cyberspace and space."[3]

In his *Chairman's Direction to the Joint Force* Chairman of the Joint Chiefs of Staff, General Martin Dempsey, outlines his priorities for the Joint Force. One of his objectives is to "Achieve our National Objectives in our Current Conflicts." In order to achieve this he outlines what are essentially lines of operations. One of which is "Prevent and mitigate the impact of a cyber-attack. Extend cyber domain awareness, establish an active defense, and provide responsible offensive capabilities."[4] This directive is precisely the kind of objectives the fundamental capabilities of the Navy's Information Dominance Corps (IDC) can be used to achieve. General Dempsey's directive also implies the necessity to achieve Information Dominance and to use information not only as an enabler but also as a means of war. There

[3] U.S. Office of the Secretary of Defense. "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense." *Department of Defense.* Department of Defense, 03 Jan 2012. p. 5.
[4] Department of Defense. Office of the Chairman of the Joint Chiefs of Staff. "Chairman's Strategic Direction for the Joint Force," 06 Feb 2012. p. 3, 5.

are multiple Navy service-level guiding documents that underscore the need to achieve Information Dominance and proposed methods for doing so. These documents include *Sea Power 21: Projecting Decisive Joint Capabilities, Navy Strategy for Achieving Information Dominance 2013-2017, U.S. Navy Information Dominance Roadmap 2013-2028,* and *Navy Cyber Power 2020.*

In the context of operational art, information can be considered as both a way and means to an end. The Navy's Chief, Information Dominance Officer has stated information has been "…historically employed as an enabler of combat (information "in" warfare), information is being deployed more and more as a weapon (information "as" warfare). Cyberspace is the information warfighting domain…information as both a weapon and an enabler in combat is driving an altogether unique warfighting capability that the U.S. Navy is calling Information Dominance."[5] Information as warfare is further clarified in the *Navy's Newest Warfighting Imperative* in which the link between cyberspace, the networks that pass through it, the people who use it, and the output that is produced combine to essentially form combat systems.[6]

U.S. Navy Information Dominance: What Is It?

The U.S. Navy defines Information Dominance as:

> The operational advantage gained from fully integrating Navy's information functions, capabilities, systems, and resources to optimize decision making and maximize warfighting effects in the complex maritime environment of the 21st Century…which are predicted to stress U.S. Navy freedom of movement and

[5] Kendall L. Card and Michael S. Rogers, Vice Admirals, USN, "Navy Strategy for Achieving Information Dominance 2013-2017: Optimizing Navy's Primacy in the Maritime Information Domains," *Public.navy.mil/fcc_c10f,* November 2012, accessed 8 March 2013, http://www.public.navy.mil/fcc-c10f/Pages/FactSheets.aspx. p. 3-4.

[6] Kendall L. Card and Michael S. Rogers, Vice Admirals, USN, "The Navy's Newest WARFIGHTING IMPERATIVE," *United States Naval Institute. Proceedings* 138, no. 10 (2012): 22-26, accessed 11 April 2013, http://search.proquest.com/docview/1115097975?accountid=322.

capabilities in future conflict.[7]

Within this definition is the very principle of Navy Information Dominance: The integration of Navy information functions and capabilities; to use them in concert with one another to maximize warfighting effects. It would not be errant to assume, based on joint warfighting concepts, that what the Navy predicts will stress its freedom of movement in information and operating environments will have a similar effect on other services of the Joint Force. The Navy expects to achieve Information Dominance by leveraging the integrated capabilities of multiple sub-communities and disciplines called the Information Dominance Corps (IDC). These communities include Oceanography, Meteorology, Information Warfare (cryptologic resources and electronic warfare), Space Cadre, Information Professionals (communications and networks), and Intelligence Professionals.[8] The Navy argues that commanders are enabled to maintain freedom of action in the information domain if three fundamental capabilities are optimized: 1) Assured Command and Control (C2), 2) Battlespace Awareness, and 3) Integrated Fires. In exercising these capabilities the IDC will provide the commander an advantage with respect to the enemy's decision cycle.[9] Elements of Assured C2 include the abilities to "exchange orders and responses with subordinates; understand the disposition of friendly forces; target and conduct strikes as part of a joint force; and assess results of those strikes."[10] Battlespace Awareness includes "persistent surveillance of the maritime and information battlespace, penetrating knowledge of the capabilities and intent of our adversaries; an understanding of when, where,

[7] William E. Leigher, Rear Admiral, USN, OPNAV Staff, Director, Warfare Integration. "U.S. Navy: Information Dominance Roadmap 2013-2028," Mar 2013. p. 1.
[8] Kendall L. Card and Michael S. Rogers, Vice Admirals, USN, "Navy Strategy for Achieving Information Dominance 2013-2017: Optimizing Navy's Primacy in the Maritime Information Domains," *Public.navy.mil/fcc_c10f*, November 2012, accessed 8 March 2013, http://www.public.navy.mil/fcc-c10f/Pages/FactSheets.aspx. p. 14.
[9] Ibid., 6.
[10] Ibid.

and how our adversaries operate; and expertise within the electromagnetic spectrum."[11] Integrated Fires summarizes the Navy's use "of its networks, cyberspace and space capabilities to exploit and attack the vulnerabilities of its adversaries to achieve non-kinetic effects (i.e., fires)."[12] History proves elements of the Navy's Information Dominance Corps can have a significant role in warfare. The Battle of Midway in June 1942 proved this with the fusion of operational intelligence and cryptology to achieve information and decision superiority over the Japanese.[13] The Navy's three fundamental capabilities to achieve Information Dominance were present at the Battle of Midway.

The Battle of Midway: A Primer

A study of the history of the Battle of Midway during World War II provides clear links between past and present Information Dominance concepts. Upon conclusion of this study one will be able to draw multiple parallels between this historical example and what today's modern Navy aims to achieve with the Information Dominance Corps, essentially proving that what the Navy is trying to achieve today with the IDC are things the Navy and military have done before, albeit in a different time and space with different technologies available to the warfighter.

Following the surprise Japanese attacks on Pearl Harbor, Hawaii on December 7th, 1941 the United States was forced into a strategic defensive position and sought to counter the Japanese desire for an expedient end to the war in the Pacific. In order to successfully do this the Commander in Chief, United States Pacific Fleet, Fleet Admiral Chester Nimitz, knew he needed to be one step ahead of the Japanese war machine, particularly the Imperial

[11] Ibid., 7.
[12] Ibid.
[13] Robert Huddleston, "Information Superiority: Paving the Way for Victory at the Battle of Midway." Information Dominance Corps Newsletter May 2012.

Japanese Navy.[14] This task would be the responsibility of Admiral Nimitz's Fleet Intelligence Officer, Captain Edwin Layton, and his Fleet Cryptologist, Commander Joe Rochefort.[15] The organization formed to synthesize the intelligence and cryptologic information on Japanese operations in the Pacific was called the Joint Intelligence Center Pacific Ocean Area (JICPOA). The predecessor to JICPOA was simply called Intelligence Center Pacific Ocean Area or ICPOA.[16] Despite its official designation after the Battle of Midway which occurred from 4-7 June, JICPOA was essentially one of the, if not the, first effective all-source intelligence unit and was situated in the Makalapa Crater at Pearl Harbor, HI.[17] As part of its all-source fusion responsibilities, JICPOA was to prepare strategic estimates for major operations by analyzing multiple sources of intelligence, including radio intercepts. JICPOA was also responsible for combat intelligence.[18] Additional intelligence organizations that contributed to JICPOAs mission were OP-20-G which was the Code and Signals Section of the Chief of Naval Operations staff in Washington D.C. and Station-HYPO which was the code breaking unit at Pearl Harbor.[19] Through the tireless efforts of these key intelligence entities, and led by Layton and Rochefort, JICPOA was able to produce intelligence estimates that successfully predicted the location, timing, and force composition of the Imperial Japanese Navy in their attack on the island of Midway. They did this through decoding intercepted radio communications and the synthesis of operational intelligence. With this intelligence Admiral Nimitz optimally positioned his numerically

[14] Patrick D. Weadon, "How Cryptology enabled the United States to turn the tide in the Pacific War," Information Dominance Corps News Letter May. 2012: p. 2.
[15] Ibid.
[16] Jeffery M. Moore, *Spies for Nimitz: Joint Military Intelligence in the Pacific War*. (Annapolis: Naval Institute Press, 2004). p. 8. JICPOA was not officially designated in writing by Admiral Nimitz until 24 June 1942.
[17] Ibid., 28.
[18] Edwin T. Layton, Rear Admiral, USN (Ret), Roger Pineau, USNR (Ret), and John Costello, "*And I Was There" Pearl Harbor and Midway-Breaking The Secrets*. (New York: W. Morrow, 1985.), p. 471.
[19] Patrick D. Weadon, "How Cryptology enabled the United States to turn the tide in the Pacific War," Information Dominance Corps News Letter May. 2012: p. 2.

inferior forces to confront the approaching Japanese naval fleet as they moved toward Midway.[20] In his order to the Fleet dated 27 May 1942, Admiral Nimitz included an "Information" section with specific details that resulted from JICPOAs intelligence efforts. Only Task Force Commanders received a "special intelligence annex," which likely contained the specific code-breaking details and assessments placing the Japanese forces in vicinity of Midway.[21] Captain Layton and Commander Rochefort, through the expertise of JICPOA, OP-G-20, and Station-HYPO, essentially provided Nimitz a time and space decision advantage; he had decision superiority because his intelligence staff had achieved Information Dominance. History shows that the principle of the Navy's current Information Dominance Corps was at play in the run up to the Battle of Midway. Although victory was surely achieved by skilled and courageous aviators, Information Dominance enabled the eventual success of the operation and was used offensively in the active targeting of radio communications which Layton and Rochefort exploited.[22]

Midway: Information Dominance and Fundamental Capabilities at Play

The principle of the Navy's current IDC and Information Dominance fundamental capabilities can be linked to actions Nimitz and his staff employed in defeating the Imperial Japanese Navy at the Battle of Midway. The fusion of operational intelligence and cryptology that provided Admiral Nimitz the necessary indications and warning to place his fleet in the best possible position to the confront the Japanese fleet is one example. The fusion of these two sub-communities, intelligence and cryptology, is one of the penultimate concepts of the IDC; maximum benefit will always be gained through collaborative efforts

[20] Ibid., 2-3.
[21] Chester W. Nimitz. 1942. CINCPAC File A16-3/(16) Operation Plan No. 29-42. United States Pacific Fleet, Pearl Harbor, HI, 27 May 1942.
[22] Robert Huddleston, "Information Superiority: Paving the Way for Victory at the Battle of Midway." Information Dominance Corps Newsletter May 2012.

from mutually supporting specialties. Similarly, the IDC's fundamental capability of Assured C2 is essential in achieving Information Dominance. In the case of Midway, Assured C2 was achieved as evidenced by Nimitz's ability to exchange orders and responses to his subordinates securely across the expansive Pacific Ocean Area.[23] His order to the Fleet, Operation Plan 29-42, provided a framework for success which was possible due to the all-source, predictive, and timely nature of the intelligence. Even more important was Nimitz's ability to disseminate the order across and down the chain of command.[24] Another fundamental capability of the Navy's current Information Dominance strategy was achieved at Midway; Battle Space Awareness. Intelligence preparation and Layton and Rochefort's cultivation of the cryptologic sources and methods in the run up to the Battle of Midway ensured Nimitz had penetrating knowledge of the capabilities and the intent of the Imperial Japanese Navy's plans to attack Midway.[25] Equally important to the intelligence successes leading to Midway was the integration of weather analysis that was added to Nimitz's decision calculus which assisted in ensuring surveillance efforts were optimized to support mission success.[26] These operational applications best depict the benefit of leveraging the various sub-communities of the Navy's current IDC of Meteorology, Oceanography, Information Warfare (cryptology), and Intelligence. Additional evidence supporting Nimitz's attainment of Battle Space Awareness can be drawn from analysis of the trust and confidence he placed in the intelligence he was receiving from Layton and Rochefort. Nimitz understood the details of the warnings he was receiving; he knew the source of the

[23] Ibid.
[24] Carl H. Builder, Steven C. Bankes, and Richard Nordin, Command Concepts: A Theory Derived from the Practice of Command and Control. 1999. p. 41.
[25] See footnote 11. Included in the IDC Fundamental Capability of Battle Space Awareness is "Penetrating knowledge of the capabilities and intent of our adversaries and an understanding of when, where, and how our adversaries operate."
[26] Robert Huddleston, "Information Superiority: Paving the Way for Victory at the Battle of Midway." Information Dominance Corps Newsletter May 2012.

information and was confident it was extremely reliable. Nimitz also knew his intelligence and cryptology staff had done the hard work of validating the sources and carefully crafted their products from this information.[27] Another enabling factor to this whole process was the value and confidence Admiral Nimitz placed on intelligence and the work of his staff.[28] His leadership style, described as "supreme cool, confidence," likely created the atmosphere in which his intelligence staff perceived the professional latitude to make bold assessments based on sound sources and methods.[29] Last, what the Joint Force would consider Integrated Fires in today's information domain would be nearly impossible to achieve at Midway simply because the advanced networks of today did not exist; however, the networks of the day (radio communication for the U.S. and Japanese) were exploited to the distinct advantage of Nimitz and his forces. In this context, one can conclude Nimitz's staff achieved a degree of Integrated Fires in the information domain that existed in May-June 1942. The parallels between the historical case study of Midway and Navy IDC capabilities of today show that the Navy's three Information Dominance fundamental capabilities were instrumental in achieving victory in war. One can examine the concept of Information Dominance as viewed by other services of today's Joint Force and see that although they contain elements of the Navy's fundamental capabilities and IDC principle; they lack one or more element(s) of the Navy's model.

Today's Joint Force and Information Dominance: We Were Better at Midway

The Midway case study showed the relevance of Information Dominance capabilities in warfare in a historical context. Today's Navy has very specific guidance and strategy for

[27] Ariel Levite, *Intelligence and Strategic Studies*. (New York: Columbia University Press, 1987.) p. 125-126.
[28] Ibid., 125.
[29] E.B. Potter interview of Layton, March 1970, Papers of Edwin T. Layton, Box 30, Folder 5, Naval Historical Collection (NHC), United States Naval War College, Newport, RI.

achieving Information Dominance, particularly in the maritime domain. While other services of the Joint Force have embraced the general concept of Information Dominance, their interpretations and application of Information Dominance principles are not as comprehensive as the Navy's model. A closer examination is warranted. Headquarters, United States Air Force (USAF) Chief for Information Dominance mission brief outlines the strategic goals and priorities for achieving Information Dominance. Among these include "Shape Cyber Force and Enable Cross-Domain Resilient Cyberspace Capabilities." The USAF aims to do this through "Cyberspace Operations and Warfighter Systems Integrations" which is centered on command and control capabilities.[30] While operating in cyberspace is certainly an element of Information Dominance and command and control is included in Assured C2, the Navy model points to a holistic approach for defensive and offensive use of information, maximizing the collaborative capabilities of sub-communities, and enabling freedom of movement not only in the maritime domain, but one could argue across elements of all domains. The USAF model for Information Dominance does not include Battlespace Awareness or Integrated Fires. The United States Army's Information Dominance Center (resident within U.S. Army Intelligence & Security Command – ISCOM) aims to provide the military commander and inter-agency representatives with time-sensitive all-source fused intelligence products.[31] Based on this information, one could assess that the primary focus of U.S. Army Information Dominance is producing actionable intelligence. The Army's goal of actionable intelligence is certainly a component of Information Dominance but it does not imply the inclusion of the expertise of sub-communities to provide a collaborative, multi-

[30] Department of the Air Force. Chief Information Officer. "SAF/CIA A6 Mission Brief," Headquarters, U.S. Air Force, Apr 2013.
[31] "INSCOM Command History." INSCOM – U.S. Army Intelligence & Security Command. Department of the Army. 25 Mar. 2013.

discipline approach; intelligence is but one component. Related to the Navy's model, the Army model will likely achieve Battlespace Awareness but lacks a comprehensive approach to achieve Assured C2 and Integrated Fires. Additionally, it does not speak to using information as a weapon or freedom of action in cyberspace.

The need for a comprehensive, Joint Force model for achieving Information Dominance is imperative to success in future conflicts. The Navy's model for achieving Information Dominance can provide that framework which will be discussed further below. However, one must first understand why IDC concepts are applicable in today's operating environment.

Why IDC Concepts are Relevant in Today's Warfighting

Analysis of the Battle of Midway proves the principle of today's IDC was just as applicable in war fighting 71 years ago. IDC concepts and desired outcomes are enduring as warfare is waged in traditional domains such as land, sea, and air and will be even more applicable as warfare continues its transition into cyberspace. In June 2011, as part of the disestablishment of the Unified Combatant Command, United States Joint Forces Command (USJFCOM), multiple resident commands/functions were transferred to existing Combatant Commands. One such command was the Joint Enabling Capabilities Command (JECC).[32] JECC's mission is to provide a deploying Joint Task Force with trained professionals who are capable of quickly integrating into a Joint Force Commander's mission battle rhythm. Information superiority and communications are elements JECC can provide to the commander upon arrival.[33] This stresses the importance the Department of Defense places on information superiority, which the IDC and its capabilities are instrumental in achieving,

[32] Donna Miles, Joint Forces Command Transfers More Functions. Lanham, United States, Lanham: Federal Information & News Dispatch, Inc, 2011.
[33] Ibid.

and is an enduring issue that must be emphasized. Additional reinforcement of the need for continued focus on building and employing Information Dominance capabilities is reflected in an observation made by U.S. Navy leadership regarding the current/near-term operational environment (2013-2019).[34] In his recent guidance issued to the Navy, Rear Admiral William Leigher, Director of Warfare Integration commented that although the Joint Force is well suited to operate in the traditional warfare domains and cyberspace, significant developments in enemy weapons employment and capabilities are leveling the playing field and, if left unchecked, will narrow the span of U.S. advantage over the adversary.[35] Information Dominance and cyberspace are inextricably linked; you cannot have one without the other. With the continued transition of warfare into the information domain, freedom of movement in this domain, just like air, sea, land and space, is just as critical and needs to be assured through Information Dominance capabilities; something the Joint Force Commander (JFC) will be obligated to consider in future conflicts. Underpinning the importance of this is the direction to U.S. Armed Forces, read Joint Force Commander, provided by the President and Secretary of Defense which highlight the critical role cyberspace operations play in the success of the Joint Force across all mission areas.[36]

With clear linkages between Information Dominance and Cyberspace established one does not have to look too far into history to find examples of information used as a weapon in cyberspace in an effort to gain an advantage in war. In the row between Russia and Estonia in the Spring of 2007, Estonian government systems were subjected to denial-of-service

[34] Department of the Navy. OPNAV Staff, Director, Warfare Integration. "U.S. Navy: Information Dominance Roadmap 2013-2028," Mar 2013.
[35] Ibid., 2.
[36] In his Defense Strategic Guidance President Obama lists "Effectively Operate in Cyber Space as a Primary Mission for U.S. Armed Forces (p.5). This is further reinforced in CJCS General Dempsey's *Strategic Direction to the Joint Force* in which he emphasized the need to "provide responsible offensive capabilities" in cyberspace (p.5).

attacks which rendered banking functions and government websites useless for extended periods of time.[37] Later, in July 2008, prior to the Russian military invasion of Georgia, multiple Georgian government and socio-economic focused web-sites were the subjects of denial-of-service attacks leaving them unusable.[38] Russia's use of information as a weapon in cyberspace likely provided them a physical and psychological advantage over their adversary. As previously discussed, the joint force arguably has an advantage in the traditional domains in today's operational environment, however this is not as true in the information environment. Navy leadership also acknowledges that the distance between U.S. capabilities and those of the adversary as they relate to "information-based capabilities" are narrowing.[39] Potential adversaries are exploiting the information environment to their own benefit. This is evidenced in the February 2013 Mandiant report, *APT1: Exposing One of China's Cyber Espionage Units.* This report details China's People's Liberation Army persistent, wide-reaching, long-standing cyber espionage efforts against some 141 organizations stealing terabytes worth of information. Mandiant further assesses that efforts by APT1 are likely sanctioned by the Chinese government, thus indicating the intent to conduct cyber operations over the long term.[40] While there can be spirited debate about whether cyber espionage constitutes a cyber-attack is irrelevant; the Chinese in this case have gained a defined level of freedom of action in cyberspace and exploited the information

[37] Tom Espiner, "Estonia's cyberattacks: Lessons learned, a year on," *ZDNet.com*, 1 May 2008, accessed 1 April 2013, http://www.zdnet/estonias-cyberattacks-lessons-learned-a-year-on_p3-303940815/.
[38] Travis Wentworth, "You've Got Malice: Russian nationalist waged a cyber war against Georgia. Fighting back is virtually impossible," *Dailybeast.com*, 22 August 2008, accessed 19 May 2013, http://www.thedailybeast.com/newsweek/2008/08/22/you-ve-got-malice.html.
[39] Department of the Navy. OPNAV Staff, Director, Warfare Integration. "U.S. Navy: Information Dominance Roadmap 2013-2028," Mar 2013. p. 2.
[40] Dan McWhorter, "APT1: Exposing One of China's Cyber Espionage Units." *Mandiant.com*, 18 February 2013, accessed 1 April 2013, https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/.

domain to their advantage. This also makes clear the need to adequately defend the information domain; a key element of Information Dominance.

The offensive cyber operations in the case of Russia and China are clear examples of exploiting the information environment to achieve Information Dominance. These are precisely the type of operations that the Joint Force Commander must defend against and be willing to use offensively when necessary.

Challenges Moving Forward: How Do We Fix It?

Once can easily draw parallels between Information Dominance and Information Superiority as prescribed by joint doctrine. That said, it is the author's belief the Joint Force could do better. Joint Warfighting in today's terms is the very essence of the military profession. The United States expects the military to operate jointly with interoperable capabilities to achieve mission success. Information Dominance is one these capabilities. While national strategic guidance, joint doctrine, and individual service guidance all agree that Information Dominance or information superiority is essential today and in future conflicts, each service has its own interpretation of how to achieve this key warfighting imperative. This must change; the Navy's model is comprehensive and can be applied to the Joint Force. In their October 2012 *United States Navy Proceedings* article entitled, "The Navy's Newest Warfighting Imperative," Vice Admirals Card and Rogers argue one must understand information dominance in an unconventional sense; information used not only to enable warfare but information to be used as a means of warfare.[41] This is a critical point in that the Joint Force Commander must think of information in a completely different light; a battery in an arsenal of tools used to protect one's own resources and center of gravity and

[41] Kendall L. Card and Michael S. Rogers, Vice Admirals, "The Navy's Newest WARFIGHTING IMPERATIVE," *United States Naval Institute. Proceedings* 138, no. 10 (2012): 22-26, accessed 11 April 2013, http://search.proquest.com/docview/1115097975?accountid=322.

use to defeat the enemy's center of gravity. "The military force that uses its networks and cyberspace to exploit and attack the vulnerabilities of its adversaries will maintain a combat advantage."[42] This is a view that must be embraced across the Joint Force. While achieving Information Dominance may mean different things as it applies to each primary warfare domain in each service, a common framework with a common set of capabilities, principles, and objectives is needed. With this new understanding comes the responsibility to comprehend, communicate, and implement Information Dominance's guiding principles and capabilities into routine operations and planning. Equally important is the requirement for the Joint Force Commander to understand where his Information Dominance resources lie, who supports them, how they are organized, and how to employ them. Although intelligence is just one component of the greater Information Dominance concept, the observations made in a 2002-2003 *Joint Force Quarterly* article entitled "Intelligence Support to Military Operations" could be applied equally to Information Dominance.[43] The author argues that demand for intelligence by military commanders will be enduring and that the Joint Force must embrace information superiority. Further, a shift in culture needs to start within the services; not solely within the national intelligence architecture.[44] This assertion speaks to the need for Information Dominance to be embraced at the service-level vice waiting for direction from higher levels of leadership; a ground-up approach to change vice top-down. Again, although focused on intelligence, this principal applies to the whole of Information Dominance.

---

[42] Kendall L. Card and Michael S. Rogers, Vice Admirals, USN, "Navy Strategy for Achieving Information Dominance 2013-2017: Optimizing Navy's Primacy in the Maritime Information Domains," *Public.navy.mil/fcc_c10f*, November 2012, accessed 8 March 2013, http://www.public.navy.mil/fcc-c10f/Pages/FactSheets.aspx. p. 4.

[43] Markus V. Garlauskas, "Intelligence Support for Military Operations." Joint Force Quarterly: JFQ.33 (2003): 102-8..

[44] Ibid., 102-103.

Information Dominance is enabled by numerous centralized and decentralized capabilities, that when combined, bring a tremendous force to bear. Central to this point is the idea that IDC professionals must be afforded the latitude to employ the principle of the IDC, and when necessary, make recommendations to the Joint Force Commander regarding the optimal use of Information Dominance defensive and, more importantly, offensive capabilities. Directly related to this is the fundamental concept of Joint Force Commander's willingness to incorporate and execute Information Dominance capabilities in his operational design. Again, using intelligence as one example of the capabilities that comprise Information Dominance, there must be openness to its utility by military commanders. In his article titled, "Why Won't They Listen? Comparing Receptivity Toward Intelligence at Pearl Harbor and Midway" Erik Dahl argues "…that the willingness of decision makers to listen to intelligence depends primarily on two factors; their belief in the seriousness of the issue or threat involved, and their trust in the utility of intelligence."[45] This observation applies to more than just intelligence; it applies to any concept that is not completely understood and traditionally not employed in warfare. If one were to reflect on the observations made in the historical example of the Battle of Midway and Admiral Nimitz's employment of Information Dominance fundamental capabilities (intelligence, cryptology, meteorology, communications) to achieve Battlespace Awareness, Assured Command & Control, and Integrated Fires, it is readily apparent his confidence in the process and its outcome enabled victory over the Imperial Japanese Navy. In E.B. Potter's biography *Nimitz,* he states, "Nimitz placed a great deal of trust in his subordinate officers and forged a team of dedicated

[45] Erik J. Dahl, "Why Won't they Listen? Comparing Receptivity Toward Intelligence at Pearl Harbor and Midway." Intelligence & National Security 28.1 (2013): 68.

professionals."[46] Speaking to the point of receptivity, employment, and outcomes of Information Dominance concepts, and referencing Nimitz's actions in the run up to the Battle of Midway, in his book entitled, *Miracle at Midway* Gordon Prange offers Admiral Raymond Spruance's observations that "…the credit must be given to Nimitz. Not only did he accept the intelligence picture but he acted upon it at once."[47] These are all clear examples of a Joint Force Commander who embraced an unfamiliar capability, validated its utility, and employed it against the enemy.

Conclusion

Information Dominance is often thought of as intangible and esoteric as related to the larger warfighting effort and tangible tools required to achieve victory. The spread of warfare, over time and space, from traditional domains to cyberspace and the information domain will bring increasing relevance to information and its use in war and as a means of war. The guidance from our civilian and military leadership makes it clear that the United States expects the military to invest in and develop information capabilities specifically to operate defensively, and when necessary offensively in cyberspace. The nation expects the military to achieve Information Dominance. The Navy's Information Dominance Corps possesses the tools with which the Navy will execute these expectations. History proves the principle of Information Dominance and its fundamental capabilities are successful in war. The example of Admiral Nimitz's actions prior to and during the Battle of Midway provide a clear example of a Joint Force Commander who recognized the utility his Information Dominance staff brought to the fight, resourced them to accomplish their mission, organized them to achieve a desired outcome, empowered them to optimally perform, trusted in their

[46] E.B. Potter, *Nimitz*, (Annapolis, MD: Naval Institute Press, 1976.) p. 34.
[47] Gordon Prange, *Miracle at Midway*, (New York: McGraw-Hill, 1982.) p. 393.

judgment, and acted upon outcomes derived from his IDC capabilities. It is recommended that the charge of today's Joint Force Commander is to apply the Navy's IDC's principals across the Joint Force to exploit the information environment and make Information Dominance an effective battery in today's warfighting arsenal. Success in any future conflict depends on it.

Bibliography

Ashmore, William C.. “Impact of Alleged Russian Cyber Attacks.” Baltic Security Defense Review 11.0 (2009): 4-40. Web. 1 Apr 2013.

Builder, Carl H., Steven C. Bankes and Richard Nordin. Command Concepts: A Theory Derived from the Practice of Command and Control. Santa Monica: RAND Corporation, 1999. Web. 29 Mar. 2013.

Card, Kendall L., and Michael S. Rogers, Vice Admiral USN. “Navy Cyber Power 2020.” *Public.navy.mil/fcc_c10f*, November 2012. Accessed 8 March 2013. http://www.public.navy.mil/fcc-c10f/Pages/FactSheets.aspx.

_____. “Navy Strategy for Achieving Information Dominance 2013-2017: Optimizing Navy’s Primacy in the Maritime Information Domains.” *Public.navy.mil/fcc_c10f*, November 2012. Accessed 8 March 2013. http://www.public.navy.mil/fcc-c10f/Pages/FactSheets.aspx.

_____. "The Navy's Newest WARFIGHTING IMPERATIVE." *United States Naval Institute. Proceedings* 138, no. 10 (2012): 22-26. Accessed 11 April 2013. http://search.proquest.com/docview/1115097975?accountid=322.

Clark, Vern. "Sea Power 21: Projecting Decisive Joint Capabilities." *United States Naval Institute. Proceedings* 128, no. 10 (2002): 32-41. Accessed 8 March 2013. http://search.proquest.com/docview/206003035?accountid=322.

Dahl, Erik J. "Why Won't they Listen? Comparing Receptivity Toward Intelligence at Pearl Harbor and Midway." *Intelligence & National Security* 28.1 (2013): 68. *ProQuest Military Collection; ProQuest Research Library.* Web. 8 Mar. 2013.

E.B. Potter Interview of Layton, March 1970, Papers of Edwin T. Layton, Box 30, Folder 5, Naval Historical Collection (NHC), Naval War College.

Espiner, Tom. “Estonia’s cyberattacks: Lessons learned, a year on.” *ZDNet.com*, 1 May 2008. Accessed 1 April 2013. http://www.zdnet/estonias-cyberattacks-lessons-learned-a-year-on_p3-303940815/.

Garlauskas, Markus V.. "Intelligence Support for Military Operations." *Joint Force Quarterly: JFQ*.33 (2003): 102-8. *ProQuest Military Collection; ProQuest Research Library.* Web. 8 Mar. 2013.

Huddleston, Robert. “Information Superiority: Paving the Way for Victory at the Battle of Midway.” Information Dominance Corps Newsletter May 2012: 4.

“INSCOM Command History.” *INSCOM – U.S. Army Intelligence & Security Command.* Department of the Army. 25 Mar. 2013. Web. 19 Apr 2013.

Layton, Edwin T., Rear Admiral, USN (Ret), Roger Pineau, USNR (Ret) and, John Costello. *"And I Was There" Pearl Harbor and Midway-Breaking The Secrets*. New York: W. Morrow, 1985.

Levite, Ariel. *Intelligence and Strategic Studies*. New York: Columbia University Press, 1987.

Markoff, John. "Before the Gunfire, Cyberattacks." *Nytimes.com,* 13 August 2008. Accessed 19 May 2013. http://www.nytimes.com/2008/08/13/technology/13cyber.html?em.

McWhorter, Dan. "APT1: Exposing One of China's Cyber Espionage Units." *Mandiant.com,* 18 February 2013. Accessed 1 April 2013. https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/.

Miles, Donna. *Joint Forces Command Transfers More Functions*. Lanham, United States, Lanham: Federal Information & News Dispatch, Inc, 2011. *ProQuest Military Collection; ProQuest Research Library.* Web. 8 Mar. 2013.

Moore, Jeffery M.. *Spies for Nimitz: Joint Military Intelligence in the Pacific War. Annapolis.* Naval Institute Press. 2004.

Nimitz, Chester W. 1942. CINCPAC File A16-3/(16) Operation Plan No. 29-42. United States Pacific Fleet, Pearl Harbor, HI, 27 May 1942. Print. 15 Mar 2013.

Potter, E.B. *Nimitz.* Annapolis, MD: Naval Institute Press, 1976.

Prange, Gordon, *Miracle at Midway,* New York: McGraw-Hill, 1982.

Scott, Chris. "Anti-Access Area-Denial (A2AD) in Military Domains and in Cyberspace." *CTOVISION.COM.* CTOVISION.COM. 17 Dec. 2012. Web. 2 Apr. 2013.

United States. Department of the Air Force. Chief Information Officer. "SAF/CIA A6 Mission Brief," *Secretary Air Force Chief Information Officer.* Headquarters, U.S. Air Force, Apr 2013. Web. 19 Apr 2013.

United States. Department of Defense. Office of the Chairman of the Joint Chiefs of Staff. "Chairman's Strategic Direction for the Joint Force," *Joint Chiefs of Staff.* Department of Defense, 06 Feb 2012. Web-PDF. 08 Mar 2013.

_____. Office of the Chairman of the Joint Chiefs of Staff. "Capstone Concept For Joint Operations: Joint Force 2020." Joint Chiefs of Staff, 10 Sep. 2012. Print. 2 Apr. 2013.

_____. Office of the Chairman of the Joint Chiefs of Staff. "Joint Publication 1: Doctrine for the Armed Forces of the United States." Joint Chiefs of Staff, 02 May 2007, Incorporating Change 1 20 Mar. 2009. Print. 20 Apr. 2013. (GL-7)

_____. Office of the Chairman of the Joint Chiefs of Staff. "Joint Publication 3-13: Information Operations." Joint Chiefs of Staff, 10 Nov. 2012. Print. 1 Mar. 2013.

_____. Office of the Secretary of Defense. "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense." *Department of Defense.* Department of Defense, 03 Jan 2012. Web-PDF. 08 Mar 2013.

United States. Department of Interior. U.S. Forestry Service. "Joint Vision 2020." *U.S. Forestry Service.* Department of Defense: Chairman of the Joint Chiefs of Staff, Director for Strategic Policy-J5, U.S. Government Printing Office, Washington DC, June 2000. Web-PDF. 08 Mar 2013.

United States. Department of the Navy. OPNAV Staff, Director, Warfare Integration. "U.S. Navy: Information Dominance Roadmap 2013-2028." Department of the Navy, Mar 2013. PDF. 29 Mar 2013.

Weadon, Patrick D. "How Cryptology enabled the United States to turn the tide in the Pacific War." Information Dominance Corps News Letter May 2012: 2-3.

Wentworth, Travis. "You've Got Malice: Russian nationalist waged a cyber war against Georgia. Fighting back is virtually impossible." *Dailybeast.com,* 22 August 2008. Accessed 19 May 2013, http://www.thedailybeast.com/newsweek/2008/08/22/you-ve-got-malice.html.